UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

Francine Simmons, individually and on behalf all others similarly situated, Plaintiff, v. Nelnet Servicing, LLC Defendant.	**CASE NO._____** **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Francine Simmons ("Plaintiff") brings this action on behalf of herself and all others similarly situated against Defendant Nelnet Servicing, LLC ("Nelnet" or "Defendant"). Plaintiff seeks to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from Nelnet. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of a data breach ("Data Breach") of highly sensitive personally identifiable information ("PII" or "Private Information") that Defendant Nelnet Servicing, LLC collected and insecurely stored on its computer network, thereby allowing third-party cybercriminals target, access, and exfiltrtate the unencrypted and unredacted names, email addresses, phone numbers, and Social Security numbers of Plaintiff and other similarly situated current and former student loan borrowers ("borrowers"), or any other person(s) whose Private Information was accessed in Nelnet's Data Breach ("Class Members").

2. Plaintiff brings this action on behalf of herself and all persons whose PII was compromised when Nelnet: a) failed to adequately protect Plaintiff's and Class Members' PII; b) did not forewarn Plaintiff and Class Members of its inadequate security practices and failure to encrypt their highly sensitive PII; c) failed to closely monitor its computer network for vulnerabilities and breaches; and d) delayed notification of the Data Breach to Plaintiff and Class, thereby increasing Plaintiff and Class Members' risk of identity theft. Nelnet's actions are unlawful, negligent, and violate federal and state statutes.

3. On its computer network, Nelnet holds and stores the Private Information of Plaintiff and putative Class Members, who are past and current student loan borrowers, as well as, upon information and belief, may also be current and former employees of Nelnet, i.e., individuals who provided their highly sensitive and private information when they began to work for Nelnet.

4. According to the Notice of Data Breach Letters that Nelnet sent to Plaintiff, Class, and the State Attorneys General, this widespread Data Breach involved the sensitive PII of 2,501,324 individuals.[1] Nelnet explained in the required notice letter that it discovered an "unknown party" gained access to a portion of Nelnet's system beginning in June 2022 and ending on July 22, 2022.[2]

5. Nelnet finally began notifying the approximately **two and a half million** victims on or about August 26, 2022, through its "Notice of Security Incident" letter, including that the "impacted information" included occurred that their PII had been stolen in what Defendant calls a "vulnerability."[3]

---

[1] Office of the Maine Attorney General, Data Breach Notifications, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml (last accessed September 7, 2022).
[2] *See, e.g.*, Exhibit A, Plaintiff's Notice Letter.
[3] *Id.*

6. Plaintiff's letter stated that her name, address, email address, phone number, and Social Security number were included in the "impacted" data. *See* Plaintiff's Notice Letter, attached as Exhibit A.

7. As a result of Nelnet's Data Breach, Plaintiff and literally millions of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the loss of their time reasonably incurred to remedy or mitigate the effects of the attack. Moreover, Plaintiff and Class Members face an imminent and substantial treat of identity theft due to the beach of their Social Security numbers along with other personally identifiable information like names, address, and dates of birth. Stolen together—and potentially sold together on the dark web—the loss of this PII can and will result in years of risk of identity theft.

8. In addition, in its Notice Letters to Plaintiff and Class Members—who entrusted their sensitive personal information to Defendant—Nelnet claims that "[t]he confidentiality, privacy, and security of our customers' information is one of our highest priorities."[4] Yet this is the same information that was left insufficiently protected, unencrypted, and was compromised in the Data Breach.

9. Upon information and belief and based upon Nelnet's notices, the Private Information compromised in the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-criminals who perpetrated this attack and remains in the hands of those cyber-criminals.

10. The Data Breach was a direct result of Defendant's failure to implement adequate

[4] *Id.*

and reasonable cyber-security procedures and protocols necessary to protect Plaintiff and Class Members' Private Information. Nelnet maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on its computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take proactive steps to secure the Private Information from those risks left that property in an unreasonably vulnerable condition.

11. Defendant disregarded the privacy and property rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

12. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the intrusion sooner, and potentially been able to mitigate the injuries to Plaintiff and the Class.

13. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, selling Class Members' data to other cybercriminals, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names

but with another person's photograph, and giving false information to police during an arrest.

14. Plaintiff and Class Members have suffered injuries as a result of Nelnet's conduct. These injuries include: a) lost or diminished value of PII; b) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; c) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, d) the loss of time needed to take appropriate measures to avoid unauthorized and reverse fraudulent charges (*e.g.,* changing usernames and passwords; investigating, correcting, and resolving unauthorized debits); e) address problems associated with spam texts, calls, and e-mails received subsequent to the Data Breach; and f) face continued and substantial risk to their PII, which remains in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

15. Plaintiff's and Class Members' personal and financial identities now face imminent and substantial risks because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff seeks remedies on behalf of herself and the Class including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant.

17. Accordingly, Plaintiff brings this action against Defendant Nelnet seeking redress for its unlawful conduct.

II. PARTIES

18. Plaintiff Francine Simmons is and at all times mentioned herein as an individual citizen of the State of Georgia, residing in the city of Tifton (Tift County). Plaintiff Simmons is a student loan borrower whose student loans are or were serviced by NelnetOn or about September 2, 2022, Plaintiff received a Notice of the Data Breach from EdFinancial regarding the Data Breach of Nelnet Servicing, LLC. A copy of the notice she received is dated August 26, 2022 and attached as Exhibit A (the "Notice Letter").

19. Defendant Nelnet Servicing, LLC is a Nebraska limited liability company that services student loans. Nelnet's principal place of business is located at 121 S. 13th Street, Suite 100, Lincoln, Nebraska 68508. Defendant can be served through its registered agent at: CT Corporation System, 5601 South 59th Street, Suite C, Lincoln, Nebraska 68516.

20. Defendant Nelnet Servicing, LLC is a wholly-owned subsidiary of Nelnet Diversified Solutions LLC, a Lincoln, Nebraska based limited liability company, which is itself a wholly-owned subsidiary of Nelnet Inc., a Lincoln, Nebraska based corporate conglomerate that serves as an administrator for the repayment of student loans and provides other education financial services.

21. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are unknown to Plaintiff at this time. Plaintiff will seek leave to amend this complaint to reflect the true names and capacities of other responsible parties if and when their identities become known.

22. All of Plaintiff's claims stated herein are asserted against Defendant Nelnet Servicing, LLC, and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

24. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in Nebraska; it is registered with the Secretary of State in Nebraska as a limited liability company; it maintains offices in Nebraska; and it committed tortious acts in Nebraska.

25. Venue is proper in this District pursuant to 28 U.S.C. § 13919b) because it is the district within which Nelnet, Inc. has the most significant contacts, Nelnet and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. STATEMENT OF FACTS

The Nature of Nelnet's Business

26. Defendant Nelnet works with the U.S. Department of Education to provide customer service on federal student loans, answering questions, assisting with deferments, and processing payments. Nelnet owns some of the loans it services, but also provides customer service and web-support for other lenders' loans, including those from the Department of Education and EdFinancial.[5]

27. Nelnet provides application processing, underwriting, fund disbursement, payment

[5] https://www.nelnet.com/your-student-loan-servicer (last accessed September 7, 2022).

processing, default aversion, and other services for its student loan portfolio and the student loan portfolios of its direct clients, including the Department of Education.[6]

28. Nelnet collects, stores, and regularly uses a vast amount of highly sensitive PII in its regular course of doing business. For example, if a borrower wants to set up a login to pay student loans, or has forgotten previously established login credentials, the very first information that must be provided to and cross-checked by Nelnet on its website is the borrower's Social Security number and birthdate, two of the most sensitive pieces of PII because neither is alterable.[7]

29. Prior to lending or servicing student loans, Nelnet requires the PII of its loan servicing customers, as well as its employees, to submit their PII, such as their names, addresses, email addresses, dates of birth, and Social Security numbers.

30. Consumers, including Plaintiff and the Class, entrusted Nelnet with their PII with the mutual understanding that Nelnet would keep this highly sensitive Private Information confidential and safeguard the information from misuse and theft.

31. In its Privacy Policy ("Privacy Policy"). Nelnet expressly promises to "implement reasonable and appropriate physical, procedural, and electronic safeguards to protect" PII placed in its care.[8] This Privacy Policy applies to any personal information provided to Nelnet and information that Nelnet collects from its website, affiliates, and mobile apps.[9]

32. Nelnet's Privacy Policy prohibits it from using and/or disclosing Plaintiff's and Class Members' Private Information unless Nelnet is complying with laws or carrying out its

---

[6] https://www.nelnet.com/privacy-and-security (last accessed September 7, 2022).
[7] *See* https://www.nelnet.com/Account/ForgotUsername and https://www.nelnet.com/Registration/Index (last accessed on September 7, 2022).
[8] https://www.nelnet.com/privacy-and-security (last accessed on September 7, 2022).
[9] *Id.*

internal loan servicing functions.[10]

33. Its Privacy Policy further claims:

> Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.[11]

34. Nelnet violated the promises it made to Plaintiff and Class in its own Privacy Policy by failing to properly secure its network such that it negligently and unlawfully disclosed Plaintiff's and Class Members' Private Information to third-party cybercriminals.

35. Plaintiff and Class Members, including current and former student loan borrowers and current and former employees, reasonably relied on the promises and policies of Nelnet to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information, as consumers, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

The Data Breach

36. According to its Notice Letters to Class Members, on July 21, 2022, Nelnet detected that unauthorized cybercriminals gained access to its information system and network. Over a month later, on or about August 26, 2022, Nelnet began notifying State Attorneys General about its widespread data breach. As Nelnet explained to the Attorneys General, its Data Breach involved

[10] *Id.*
[11] *Id.*

the sensitive PII of 2,501,324 individuals. [12]

37. Nelnet's Notice Letters admit that the Data Breach began on an undisclosed date in June 2022 and continued until July 22, 2022.[13]

38. Despite learning about the Data Breach in July 2022, when cyber criminals had already accessed the PII of Plaintiff and Class for a month or more, Nelnet chose not to notify affected Class Members for more than a month. Finally, on August 26, 2022, Nelnet admitted that Class Members' PII had been impacted and taken from its network.[14] Therefore, Plaintiff's and Class members' PII was in the hands of cybercriminals for about two months before they were notified of Nelnet's Data Breach.

39. Time is of the essence when trying to mitigate against identity theft after a data breach, so the earliest possible notification is critical, especially where highly sensitive PII like Social Security numbers paired with dates of birth are involved.

40. Because of this targeted cyberattack, and as a direct result of Nelnet's failure to adequately secure its computer network, data thieves were able to gain access to and exfiltrate data from Nelnet that included the Private Information of Plaintiff and Class Members.

41. The files exfiltrated from Nelnet contained at least the following information of Plaintiff and Class Members: names, addresses, email addresses, phone numbers, and Social Security numbers. Plaintiff and Class members likely provided Nelnet with their dates of birth (required for setting up an account or lost login information) and payment information although

---

[12] Office of the Maine Attorney General, Data Breach Notifications, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml (last accessed September 7, 2022).
[13] *See* Plaintiff's Notice Letter, Exhibit A.
[14] *See* Plaintiff's Notice Letter, Exhibit A.

Nelnet did not disclose [15]

42. Upon information and belief, the Private Information stored on Nelnet's network was not encrypted.

43. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff reasonably believes her stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information, like Nelnet does.

44. As a result of the Data Breach, Nelnet now tries to shirk its responsibilities and instructs Plaintiff and Class Members of "Steps You Can Take to Help Protect Personal Information" and also encourages Class Members to enroll in credit monitoring and identity theft restoration services.[16]

45. That Nelnet is encouraging Plaintiff and Class Members to enroll in credit monitoring and identity theft restoration services is its direct acknowledgment that the impacted Plaintiff and Class are subject to a substantial and imminent threat of fraud and identity theft.

46. Although Nelnet is offering some or all Class Members two years of credit monitoring and identity theft protections services, this offer is woefully inadequate as 1) student loan borrowers are likely to be relatively recently, well-educated adults who are just beginning to build their careers and their financial reputations, and, therefore, 2) they are likely to spend years if not decades trying to mitigate the harms caused by the breach of Nelnet's computer systems.

47. Nelnet had obligations created by contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from

---

[15] *See* Plaintiff's Notice Letter, Exhibit A.
[16] Notice Letter, Exhibit A.

unauthorized access and disclosure. Nelnet failed to meet these obligations.

48. Nelnet could have prevented this Data Breach by, among other things, properly encrypting and otherwise properly securing its equipment and computer files containing PII.

49. By obtaining, collecting, and using Plaintiff's and Class Members' PII for its own financial gain and business purposes, Nelnet assumed legal and equitable duties and knew that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach was a
Foreseeable Risk of which Defendant was on Notice

50. It is well known that PII, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of hackers. Companies that collect such information, including Nelnet, are well aware of the risk of being targeted by cybercriminals.

51. Individuals place a high value not only on their PII, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

52. Individuals, like Plaintiff and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

53. Data Breach victims suffer long-term consequences when their social security numbers are taken and used by hackers. Even if they know their social security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse.

54. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will

have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[17]

55. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[18]

56. In light of high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Nelnet knew or should have known that its computer network would be targeted by cybercriminals.

57. Cyberattacks like the one here have become so notorious that the FBI and U.S. Secret Service have issued warnings to potential targets so they are aware of, and can prepare for, and hopefully ward off any attempted cyberattacks.

58. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Nelnet failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

At All Relevant Times Nelnet Had a Duty to Plaintiff and Class Members to Properly Secure Private Information

[17] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed August 31, 2022).
[18] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed August 31, 2022).

59. At all relevant times, Nelnet had a duty (and was aware of that duty as it states in its Privacy Policy) to Plaintiff and Class Members to properly secure PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Nelnet became aware that their PII may have been compromised.

60. Upon information and belief, Nelnet had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Nelnet breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

61. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;
b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
c. Monitoring for suspicious or irregular traffic to servers;
d. Monitoring for suspicious credentials used to access servers;
e. Monitoring for suspicious or irregular activity by known users;
f. Monitoring for suspicious or unknown users;
g. Monitoring for suspicious or irregular server requests;
h. Monitoring for server requests for PII;
i. Monitoring for server requests from VPNs; and
j. Monitoring for server requests from Tor exit nodes.

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

63. The ramifications of Nelnet's failure to keep Plaintiff and Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and with names and dates of birth, fraudulent use of that information and damage to victims including Plaintiff and the Class may continue for years.

The Value of Personal Identifiable Information

64. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[21]

65. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

66. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an

---

[19] 17 C.F.R. § 248.201 (2013).
[20] *Id.*
[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed August 31, 2022).
[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/(last accessed August 31, 2022).

individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

67. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

69. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than

---

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed August 31, 2022).

[24] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed August 31, 2022).

10x on the black market."[25]

70. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[26]

71. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' PII can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

72. The information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

73. Plaintiff and Class will suffer injuries from Nelnet's Data Breach for years to come, particularly in light of the PII at issue here.

74. The injuries to Plaintiff and Class Members were directly and proximately caused by Nelnet's failure to implement or maintain adequate data security measures for current and former loan servicing consumers and employers.

Nelnet Failed to Comply with FTC Guidelines

75. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and

---

[25] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed September 7, 2022).

[26] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (last accessed September 7, 2022).

financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[27]

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[28] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

77. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[29]

78. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.
b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.
c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a

[27] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[28] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business
[29] FTC, *Start With Security*, *supra* note 28.

business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

79. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. Because Class Members entrusted Nelnet with their PII, Nelnet had, and has, a duty to the Plaintiff and Class Members to keep their PII secure.

81. Plaintiff and the other Class Members reasonably expected that when they provide PII to Nelnet (or to Nelnet's customers), Nelnet would safeguard their PII.

82. Nelnet was at all times fully aware of its obligation to protect the personal and financial data of current and former employees and consumers, including Plaintiff and members of the Class. Nelnet was also aware of the significant repercussions if it failed to do so. Its own Privacy Policies, quoted above, acknowledges this awareness.

83. Nelnet's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' first names, last names, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Nelnet's Inadequate Security and the Data Breach It Allowed.

84. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

85. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. Plaintiff and other reasonable potential customers as well as current and former customers of Nelnet understood and expected that, as part of that business relationship, they would

receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

86. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

87. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

88. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

89. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the

value of their PII, for which there is a well-established national and international market.

90. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

91. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[30] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

92. As a result of the Data Breach, Plaintiff and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

93. Defendant openly admits that its investigation shows that Plaintiff's and Class Members' highly personal PII, including Social Security numbers, was "impacted" in its Data Breach.

94. Although Nelnet attempts to hedge whether the cybercriminals actually exfiltrated the PII that was accessed, it is highly unlikely that thieves went to the trouble to break in, yet then

---

[30] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

walked away empty-handed.

Plaintiff's Experience

95. Plaintiff Francine Simmons is, and at all times relevant to this complaint, a resident and citizen of the State of Georgia.

96. Prior to the Data Breach, Plaintiff Simmons received a student loan through EdFinancial. That loan is being serviced by Defendant Nelnet. She reasonably believed that EdFinancial and Nelnet maintained a secure network to protect her and other borrowers' PII.

97. In the course of her loan application and establishing the servicing of the loan she received, Plaintiff Simmons was required to supply EdFinancial and Nelnet with her PII, including but not limited to her name, address, email address, phone number, date of birth, Social Security number, and financial account information. At the time that she provided this private information, she was assured and likewise assumed it would be protected by EdFinancial Nelnet.

98. Beginning in about June or July of 2022, Plaintiff Simmons noticed she was receiving a significant number of spam emails and phone calls every day, sometimes multiple in a day. Prior to that time, she rarely received this sort of spam. She reasonably believes these unwanted and intrusive communications, which take time out of every day, are related to Nelnet's Data Breach since they began after the time of the Breach. Plaintiff is concerned that the spam calls and emails are being placed with the intent of obtaining more personal information from her and committing identity theft by way of a social engineering attack.

99. On or about July 4, 2022, Plaintiff Simmons received a phone alert from her credit union notifying her of fraudulent charges that were being flagged on her account. Over the next few days, she was required to spend time making sure the charges were properly reversed or denied and getting a new card for her credit union account. If not for Nelnet's Data Breach, she would not have had to spend her time resolving this identity theft incident.

100. Then on September 2, 2022, Plaintiff Simmons received the Notice of Data Breach letter, which indicated that Nelnet had known about the Data Breach for months before notifying her about the Breach. Furthermore, her Notice letter arrived several months after cybercriminals first had access to Nelnet's computer network. Had Nelnet provided her with a timely Notice of the Data Breach, she would have had additional time to be aware of and mitigate her risk of identity theft.

101. In response to Nelnet's Notice of Data Breach, Plaintiff spends time dealing with the consequences of the Data Breach, which included and will continue to include time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts including having automated alerts sent for potentially fraudulent activities. She spends time every day of every week trying to closely monitor her accounts to detect and prevent fraudulent activities. The time she is forced to spend monitoring and securing her accounts has been lost forever and cannot be recaptured. Plaintiff spent this time at Defendant's direction. Specifically, in the Notice letter Plaintiff received, Nelnet directed Plaintiff to take steps to mitigate her losses, encouraging her to "remain vigilant against incidents of identity theft and fraud over the next 24 months, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

102. Plaintiff is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

103. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided Nelnet with her PII had Nelnet disclosed that it lacked data security practices adequate to safeguard PII.

104. Plaintiff suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to EdFinancial and Nelnet for the

purpose of securing a student loan, which was compromised by the Defendant's lax security and the resulting Data Breach.

105. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Nelnet obtained from Plaintiff; (b) violation of her privacy rights; (c) the theft of her PII; and (d) imminent and substantial injury arising from the increased risk of identity theft and fraud.

106. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

107. Plaintiff Simmons reasonably believes that her Private Information may have already been sold by the cybercriminals. Had she been notified of Nelnet's breach in a more timely manner, she could have attempted to mitigate her injuries.

108. Plaintiff has a continuing interest in ensuring that her PII, which upon information and belief remains backed up and in Nelnet's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

109. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

110. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was maintained on Defendant Nelnet's computer systems and compromised in its June-July 2022 Data Breach.

111. Excluded from the Class are Defendant's officers and directors, and any entity in

which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

112. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

113. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of persons whose data was compromised in Data Breach.

114. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

115. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

116. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

117. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' Private Information

was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

118. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

119. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

120. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect its data systems were reasonable in light

of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

121. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Nelnet.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiff and Class Members)

122. Plaintiff re-alleges and incorporates by reference the paragraphs above as if fully set forth herein.

123. Nelnet owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

124. Plaintiff and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information.

125. Nelnet had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

126. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable

means to secure and safeguard its computer network—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

128. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

129. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII; and

e. Failing to detect in a timely manner that Class Members' PII had been compromised.

130. It was foreseeable that Defendant's failure to use reasonable measures to protect

Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

131. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

132. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, and an imminent and substantial risk of harm that will be suffered by Plaintiff and the Class.

133. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

134. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

135. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiff and Class Members)

136. Plaintiff re-allege and incorporate by reference the above allegations.

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

138. Nelnet violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the PII at issue in this case—including Social Security numbers.

139. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

140. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

141. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

142. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not

limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

143. Additionally, as a direct and proximate result of Defendants' negligence per se, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

144. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to Nelnet's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

145. Nelnet's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information.

146. Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Nelnet's conduct. Plaintiff and Class Members seek damages and other relief as a result of Nelnet's negligence.

THIRD COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and Class Members)

147. Plaintiff re-alleges and incorporates by the paragraphs above as if fully set forth herein.

148. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their employment relationship and/or as a condition of receiving other services provided by Defendant.

149. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for Nelnet's services or employment. In exchange for the PII, Defendant promised to protect their PII from unauthorized disclosure.

150. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

151. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

152. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

153. When Plaintiff and Class Members provided their PII to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant

agreed to reasonably protect such information.

154. Defendant required Class Members to provide their PII as part of Defendant's regular business practices.

155. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

156. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

157. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

158. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

159. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

160. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

161. Plaintiff and Class Members are also entitled to nominal damages for the breach of implied contract.

162. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide

adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and Class Members)

163. Plaintiff restates and realleges the paragraphs above as if fully set forth herein.

164. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of the provision of their PII and Defendant would be unable to engage in its regular course of business without that PII.

165. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

166. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

167. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

168. Defendant acquired the PII through inequitable means in that it failed to disclose

the inadequate security practices previously alleged.

169. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

170. Plaintiff and Class Members have no adequate remedy at law.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

172. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

173. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: September 8, 2022

Respectfully submitted,

/s/Jason S. Rathod
Jason S. Rathod*
Nicholas A. Migliaccio*
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, D.C. 20002
Office: (202) 470-3520
Fax: (202) 800-2730
www.classlawdc.com

Gary E. Mason**
Danielle L. Perry**
Lisa A. White**
MASON LLP
5301 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Email: gmason@masonllp.com
Email: dperry@masonllp.com
Email: lwhite@masonllp.com

Attorneys for Plaintiff

* permanently admitted to practice in D. Neb.

** *pro hac vice* anticipated